Begrijp onverwachte MAC-learning op Catalyst 9000 Series Switches

Inhoud

Inleiding

Dit document beschrijft een scenario waarin een Catalyst 9300 access switch een upstream MAC-adres op een downstream poort leerde.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- LAN-switching
- MAC-adresleren
- Verificatiesessies en aanverwant gedrag

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Catalyst 9300 Series switches
- Software versie 17.6.5

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

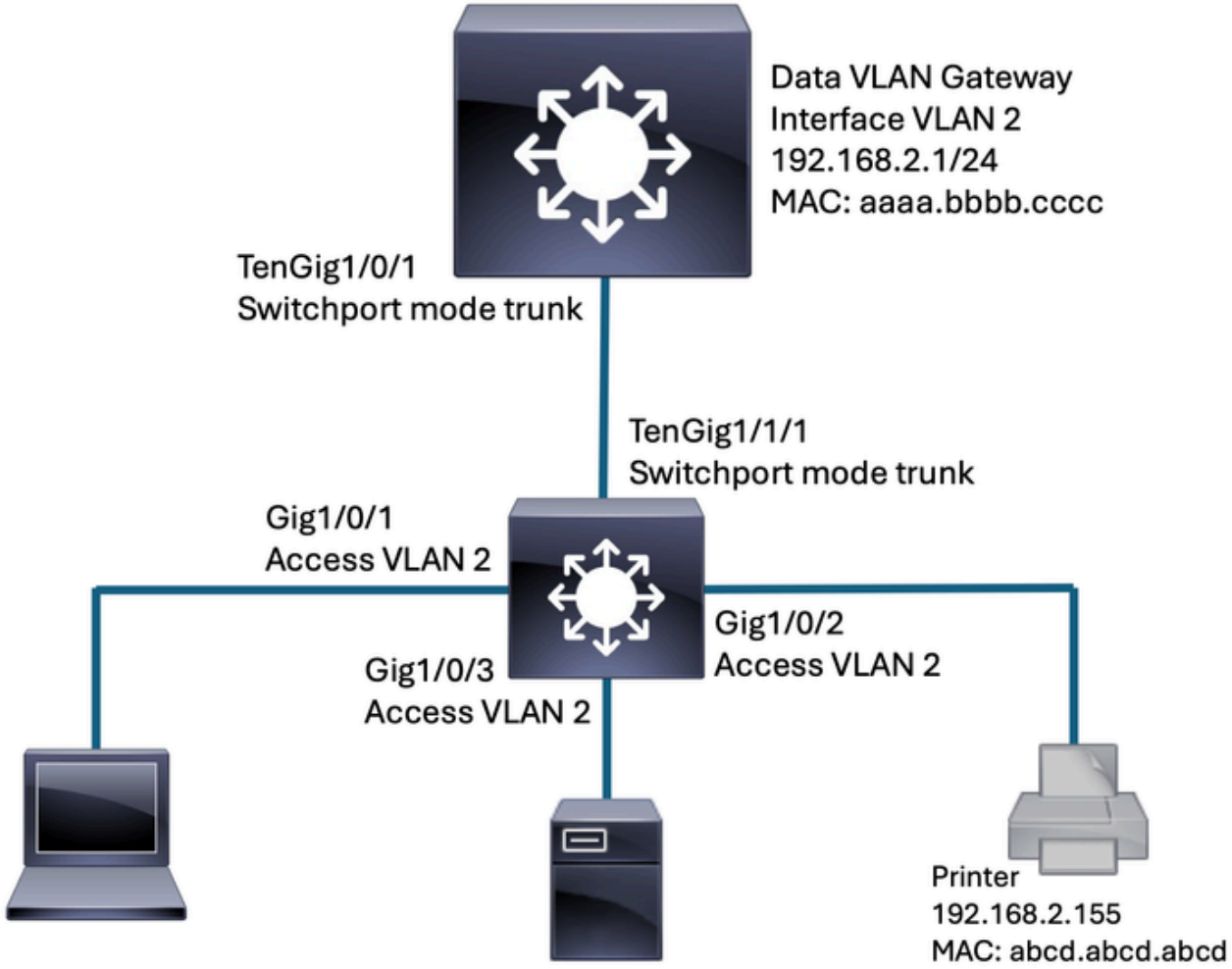
Achtergrondinformatie

Catalyst switches leren MAC-adressen op switch-poorten op basis van het MAC-bronadres (SMAC) van een inkomend frame. De MAC-adrestabel is doorgaans een betrouwbare bron van informatie die een netwerkingenieur naar de locatie van een bepaald adres leidt. Situaties ontstaan wanneer verkeer vanuit een bepaalde bron - een eindpunt of zelfs de gateway van het lokale netwerk - een switch vanuit een onverwachte richting ingaat. Dit document beschrijft een specifieke situatie waar het upstream gateway MAC-adres onverwacht werd geleerd op willekeurige toegangsinterfaces. De details zijn gebaseerd op TAC-cases die zijn opgelost door TAC-engineers die samenwerken met de teams van de klant.

Probleem

De client in dit scenario merkte eerst het probleem op wanneer endpoints in hun data VLAN (VLAN 2 in deze demonstratie) connectiviteit verloren aan hosts buiten hun subnetverbinding. Bij nadere inspectie merkten ze op dat het MAC-adres van de VLAN 2-gateway werd geleerd op een gebruikersinterface in plaats van op de verwachte interface.

Het probleem leek in eerste instantie op willekeurige wijze te gebeuren in een groot netwerk dat uit meerdere campussen bestond. Gezien wat we weten over hoe de switches MAC-adressen leren, gingen we uit van een pakketreflectie, maar de uitdaging was om te bewijzen dat het probleem buiten de switch lag. Na het verzamelen van aanvullende gegevens over andere keren dat dit probleem zich had voorgedaan, konden we een trend identificeren met de betrokken gebruikershavens. Bij elk optreden was een specifiek model van het eindpunt betrokken.



Segment van getroffen netwerk

De opdracht "show mac address-table <address>/<interface>" wordt gebruikt om de MAC-adrestabel op te vragen. In het werkende of normale scenario, dat het gatewayadres op Ten1/1/1 van de switch wordt geleerd waar de eindpunten verbinden.

<#root>

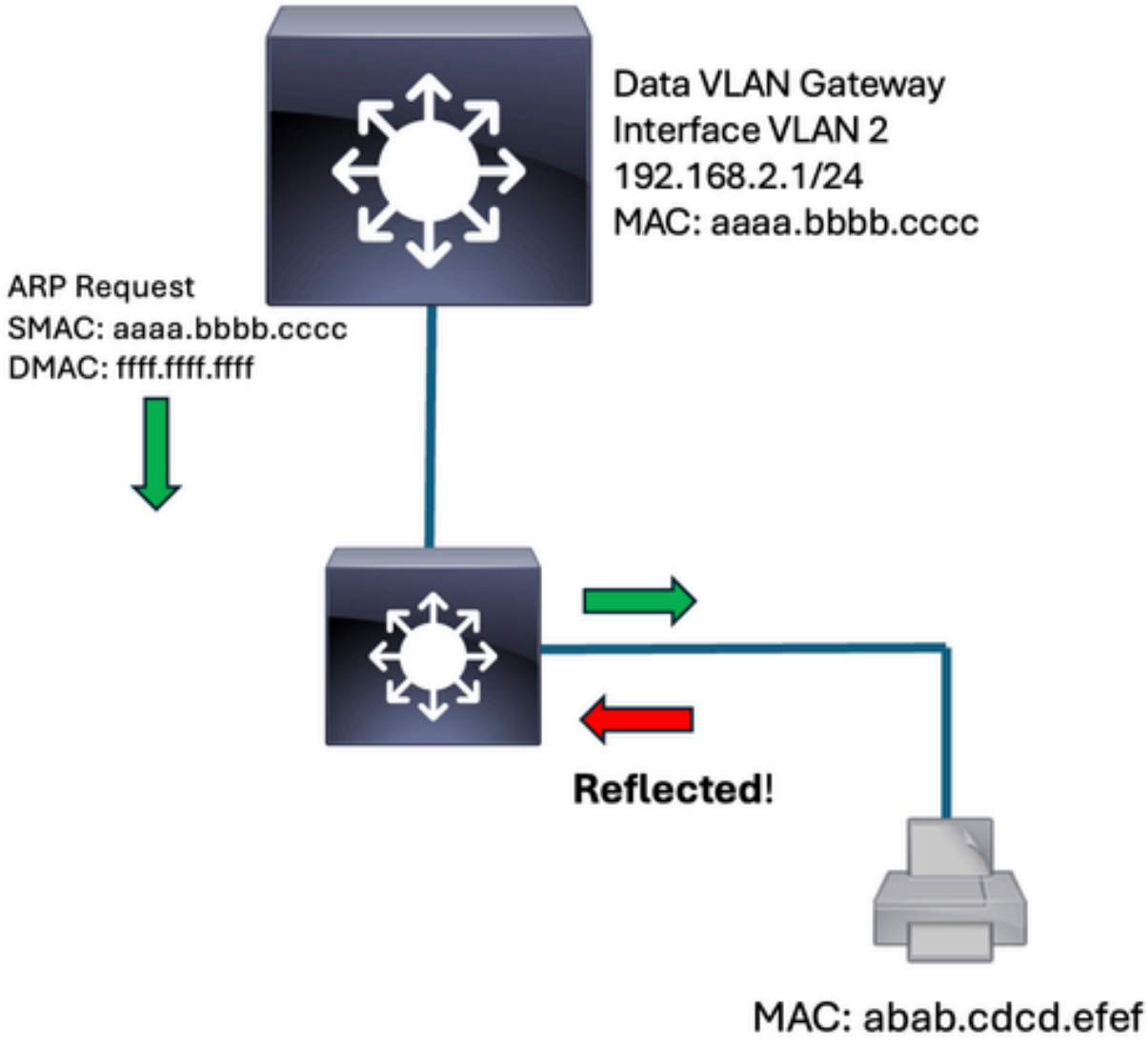
```
ACCESS-SWITCH#

show mac address-table

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 <snip>
   2    aaaa.bbbb.cccc    DYNAMIC     Ten1/1/1 <-- Notice the "type" is DYNAMIC. This means the entry wa
   2    abcd.abcd.abcd    STATIC      Gig1/0/2 <-- In contrast, this MAC is STATIC. This suggests a feat
```

In het gebroken scenario werd de gateway MAC geleerd op Gi1/0/2 en niet op Te1/1/1.

<#root>

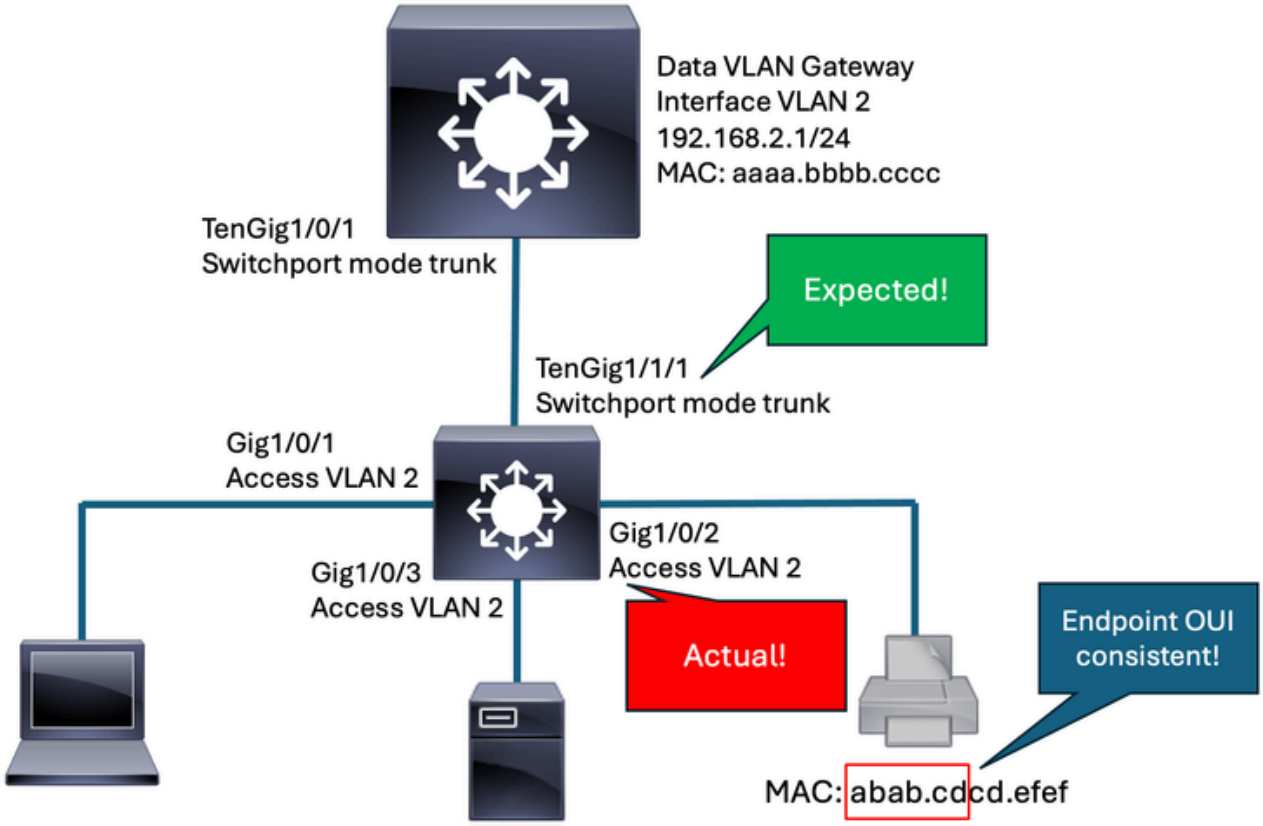
```
ACCESS-SWITCH#

show mac address-table

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 <snip>
   2    aaaa.bbbb.cccc    STATIC      Gig1/0/2 <-- Notice that the type is now STATIC.
   2    abcd.abcd.abcd    STATIC      Gig1/0/2
```

De access switch in dit scenario voert 802.1x met MAB (MAC-verificatie omzeilen) fallback op zijn toegangsinterfaces uit. Deze belangrijke kenmerken speelden een rol in de algemene impact van de dienst. Zodra het gateway MAC-adres op een toegangshaven werd geleerd, zou het 'statisch' worden als functie van de beveiligingsfunctie. De veiligheidseigenschap verhinderde ook het adres van gatewayMAC terug naar de correcte interface te bewegen. Informatie over 802.1x, MAB en het concept 'mac-move' wordt verder onderzocht in de betreffende configuratiehandleiding.



Demonstratie van gereflecteerd verkeer

De pakketreflectie leidt tot de abnormale MAC leer.



Dit diagram benadrukt de verwachte versus daadwerkelijke interface die GW MAC leert.

In het voorbeeld wordt de unieke organisatorische identificatiecode (OUI) benadrukt. Dit hielp het team identificeren dat het eindpunt van een gemeenschappelijke fabrikant was.

Oplossing

De kern van dit probleem was het onverwachte gedrag bij het eindpunt. We verwachten nooit dat een eindpunt verkeer terug in het netwerk weergeeft.

De belangrijkste bevinding in dit geval was de trend met de eindpunten. Het is moeilijk om een probleem op te lossen dat willekeurig in een groot netwerk voorkomt. Dit gaf het team een subset van gebruikershavens om te onderzoeken.

Merk ook op dat de betrokken echtheidskenmerken (namelijk dot1x met MAB fallback) een rol speelden bij de service impact. Zonder deze eigenschappen die aan het weerspiegelde verkeer beantwoorden, zou de dienstimpact waarschijnlijk niet zo groot zijn geweest.

Packet-opnametools zijn ingezet om te identificeren dat verkeer echt werd weerspiegeld door het eindpunt. Het ingesloten pakketopnamegereedschap (EPC) dat beschikbaar is op Catalyst-switches kan worden gebruikt om inkomende pakketten te identificeren.

<#root>

```
Switch#
```

```
monitor capture TAC interface gi1/0/2 in match mac host aaaa.bbbb.cccc any

Switch#
monitor capture TAC start

<wait for the MAC learning to occur>
Switch#
monitor capture TAC stop
Switch#
show monitor capture TAC buffer
```

Physical SPAN (switch port analyzer) is een betrouwbaar pakketopnameprogramma dat ook in dit scenario kan worden gebruikt.

```
<#root>
Switch(config)#
monitor session 1 source gi1/0/2 rx

Switch(config)#
monitor session 1 filter mac access-group MACL
 <- Since we know the source MAC of the traffic we look for, the SPAN can be filtered.
Switch(config)#
monitor session 1 destination gig1/0/48
```

Het team kon weerspiegeld verkeer op een haven vangen waar een verdacht eindpunt verbond. In dit scenario zou het eindpunt ARP-pakketten weerspiegelen die afkomstig zijn van het MAC-adres van de gateway, terug in de switch. De MAB-enabled switch poort zou proberen om het gateway MAC-adres te authenticeren. Dankzij de switch-poortbeveiliging kon de gateway-MAC in de gegevens-VLAN autoriseren. Aangezien het adres van MAC in combinatie met de veiligheidseigenschap werd geleerd, zou het als STATISCHE MAC op de gebruikershaven "plakken". Ook, omdat de beveiligingsimplementatie de MAC-adresbeweging van geautoriseerde MAC-adressen blokkeerde, kon de switch de MAC op de gebruikershaven niet vergeten en kon hij deze niet opnieuw leren op de verwachte interface. De pakketreflectie verergerd door de security implementatie leidde tot een situatie waarin verkeer werd beïnvloed voor het gehele lokale VLAN.

Volgorde van gebeurtenissen:

1. MAC's worden geleerd op de verwachte interfaces. Dit is de normale status van het netwerk.

2. Endpoint weerspiegelt verkeer dat afkomstig is van gateway terug naar de poort die verbinding maakt met de switch.

3. Vanwege de implementatie van de endpoint switch-poortbeveiliging, activeert de weerspiegelde MAC een verificatiesessie. De MAC is geprogrammeerd als een STATISCHE ingang.

4. Zodra de MAC uit de verwachte switch-poort is vertrokken, voorkomt de beveiligingsimplementatie dat deze op de uplink opnieuw wordt aangeleerd.

5. De haven moet gesloten/gesloten zijn om te kunnen herstellen.

De ultieme oplossing voor deze situatie was om het eindpuntgedrag aan te pakken. In dit scenario was het gedrag al bekend bij de endpointverkoper en werd het opgelost met een firmware-update. De Catalyst switch hardware en de software en configuratie gedroegen zich allemaal zoals verwacht.

De belangrijkste afleiding van dit scenario is het concept van MAC-leren. Catalyst switches leren MAC-adressen op toegang op basis van het MAC-adres van de bron van het ontvangen frame. Als een MAC-adres op een onverwachte interface wordt geleerd, is het veilig om te concluderen dat de switch-poort een frame op toegang heeft ontvangen met dat MAC-adres in het veld bron-MAC.

In zeer beperkte situaties kunnen pakketten worden weerspiegeld tussen de fysieke interface en de doorsturen ASIC van de switch - of door een ander intern wangedrag. Als dit het geval lijkt te zijn en er geen bestaande bug wordt gevonden die het probleem verklaart, neem dan contact op met TAC om te helpen met isolatie.

Gerelateerde informatie

- Packet Capture configureren - Catalyst 9300
- SPAN en RSPAN configureren - Catalyst 9300
- Probleemoplossing voor Mac Address Table Manager op Catalyst 9000 Series Switches
- IEEE 802.1x-poortgebaseerde verificatie configureren - Catalyst 9300
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.